Notice of Allowability	Application No.	Applicant(s)	
	10/785,025	SOVIO ET AL.	
	Examiner	Art Unit	
	Evens Augustin	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 08/08/2006*.

2. ☒ The allowed claim(s) is/are *1-26 and 33-49*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Status of Claims

1. Claims 1-26 and 33-49 have been examined.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joe Redmond on 27th of October 2006.

The Application has been amended as follows:

1. (Currently Amended) A method enabling a user in a mobile environment to conduct transactions via a self-service merchant terminal, comprising:

a) maintaining a security key in a mobile phone device;

b) transferring ~~imprinting~~ ~~at least an association of~~ the security key and mobile phone identification into at least one user portable fob or pilot via an initial short-range radio link;

c) transferring ~~at least the association of~~ the security key and the mobile phone identification from the at least one user portable fob or pilot to a self-service merchant terminal through the initial short-range radio link; ~~and~~

d) establishing a secure short-range connection between the self-service terminal and the mobile phone based on the transferred security key and the mobile phone identification information from the at least on user portable fob or pilot, wherein the initial short-range radio link has a significantly smaller radio coverage than the secure short-range connection, and

e) verifying the presence of a correct pilot by the terminal via computing and comparing an expected response from the mobile phone with the transferred security key

19. (Currently Amended) A system for enabling a user in a mobile environment to conduct transactions via a self-service terminal, comprising:

a) a mobile device including a short-range communication transceiver and an RFID transceiver;

b) a semi-passive RFID transponder;

c) a self-service terminal including a RFID transceiver and a short-range transceiver;

d) means for storing identification information and at least security information in the mobile device;

e) means for transferring ~~imprinting~~ said stored identification and ~~at least an association of~~ the security information of the device over an RFID connection into the user portable fob or pilot;

f) means for transferring by the user fob or pilot said transferred ~~imprinted~~ identification and security information to the self-service terminal over an RFID connection; ~~and~~

g) means for establishing a secure short-range connection between the self-service terminal and the device based on said transferred identification and security information of the device from the user portable fob or pilot, wherein the RFID connection has significantly smaller radio coverage than the secure short-range connection, and

h) means for verifying the presence of a correct pilot by the terminal via computing and comparing an expected response from the mobile phone with the transferred security key

33. (Currently Amended) A medium, executable in a computer system, enabling a user in a mobile environment to activate a self-service terminal to conduct transactions, the medium comprising:

a) program code for storing at least a security key in a mobile phone device;

b) program code for transferring ~~imprinting at least an association of~~ the security key and mobile phone device identification in a user portable fob or pilot associated with the mobile phone device;

c) program code for transferring ~~at least the association of~~ the security key and the mobile phone identification from the at least one user portable fob or pilot to a self-service merchant terminal through the initial short-range radio link; ~~and~~

d) program code for establishing a secure short-range connection between the self-service terminal and the mobile phone based on the transferred security key and the mobile phone identification information from the at least on user portable fob or pilot, wherein the initial short-

range radio link has a significantly smaller radio coverage than the secure short-range connection, and

e) program code for verifying the presence of a correct pilot by the terminal via computing and comparing an expected response from the mobile phone with the transferred security key

37. (Currently Amended) A method of enabling a first user portable fob or pilot device to serve as a master fob or pilot for at least one second user portable fob or pilot devices as slave devices capable of interacting with a terminal, comprising:

installing a reader and switching means in a first user portable fob or pilot device serving as a master device and further including a processor and storage means;

transferring ~~imprinting~~ and storing in the master fob or pilot device a phone address and a security key of a mobile phone;

at least one second user portable fob or pilot device, each serving as a slave device to the master device and further including a processor and storage, each slave device capable of receiving and transmitting signals from/to the master device;

transferring ~~imprinting~~ the phone address, security key and policy restraints in a slave device after receiving an address identifying the slave device; and

using the slave device to interact with a terminal to purchase an item, after a secure connection is established between the terminal and the mobile phone

49. (Currently Amended) A method enabling a user in a mobile environment to conduct transactions via a self-service merchant terminal, comprising:

a) maintaining a security key in a mobile phone device;

b) transferring ~~imprinting at least an association of~~ the security key and mobile phone identification into at least one user portable fob or pilot via a RFID connection between the mobile phone device and the at least associated portable pilot;

c) transferring ~~at least the association of~~ the security key and the mobile phone identification from the at least one user portable fob or pilot to a self-service merchant terminal via a RFID connection between the mobile phone device and the at least associated portable pilot;

d) establishing a secure short-range connection between the self-service terminal and the mobile phone based on the transferred security key and the mobile phone identification information from the at least on user portable fob or pilot, wherein the RFID connection has a significantly smaller radio coverage than the secure short-range connection,

e) storing a plurality of authentication codes for one time use in the device for establishing short-range connections between the device and the terminal; and

f) receiving a user transaction interface at the terminal upon establishment of the secure short-range connection

3. Claims 1-26 and 33-49 have been allowed

Reasons for Allowance

4. The present application is directed to a electronic payment schemes in a mobile environment for secure short-range transactions. The invention uses a fob or pilot device to make transaction, and the fob and pilot device is authenticated by wireless phone. The authentication takes place in this manner:

1. When becomes in contact with a kiosk or POS or self service terminal, the fob sends the device address of the mobile phone to the kiosk or Point Of Sale (POS) or self service terminal, by means of an initial proximity RFID channel connection
2. By using this address, the self-service terminal connects to the phone using a short-range radio connection, such as, for example a Bluetooth connection or the like
3. The phone generates a random nonce and sequence number SEQ and sends them to the self-service terminal via a Bluetooth connection or the like
4. The terminal sends the nonce and SEQ to the pilot via the proximity RFID channel connection
5. The pilot computes a message response and sends it to the terminal as a response message, the response being a way function based on cryptographic hash computations
6. The terminal establishing a secure short-range connection with the phone
7. The terminal verifying the presence of a correct pilot by the terminal via computing and comparing an expected response from the mobile phone with the transferred security key

The aspect using key fobs to make transactions is well know in the art (U.S. 7093767), but they are not being authenticated by cell phones (think mobile speedpass by Exxon). The aspect of using phone to make transactions is also well known in the art (U.S. 6078806, US 20040243519). In fact, the prior art (U.S. 6078806) teaches the aspect of wireless phone, in tandem with a smart card, to make transaction. In this case the phone ends up making the transaction with a POS, not the smartcard, which would be considered a pilot device. But the cell phones are not being used as an authentication means for authenticating a pilot device that would end up making a transaction with a POS devices.

The closest prior art by Zalewski et al. (U.S 6771981), which has same assignee as the claimed invention, discloses an invention that describes a **changeable cover for an electronic device**, such as a wireless phone, and a method of using the same in an electronic payment system. The **cover has an RFID transponder to communicate with POS devices** (column 8, lines 2-3). When the cover (in this case would be equivalent to a pilot device) is in the proximity of an appropriate POS device, the device is interrogated and **provides the device with information such as electronic identification mobile station phone number and the like** (column 11, lines 48-51). Even though the prior art teaches that the POS terminal communicates the wireless device/phone by sending the wireless messages such as thanking the customer for shopping with the vendor and offering some incentive to visit their convenience store at a later date (column 11, lines 62-67), and **according to Zalewski et al., the POS device does not further authenticate the ID and secret received from the pilot device, using the wireless**

device, by **comparing an expected response from the mobile phone with the transferred security key.** It also would not obvious have been obvious to use a wireless device to authenticate a fob or pilot device in the manner describe in the claimed invention.

Therefore, the present apparatus and method is distinguished from the prior art as the prior art does not teach nor fairly suggest an invention in which a fob/pilot sends a device address of the mobile phone to the kiosk or Point Of Sale (POS) or self service terminal, by means of an initial proximity RFID channel connection, and by using this address, the self-service terminal connects to the phone using a short-range radio connection, such as, for example a Bluetooth connection or the like, and the phone generates a random nonce and sequence number SEQ and sends them to the self-service terminal via a Bluetooth connection or the like, and the terminal sends the nonce and SEQ to the pilot via the proximity RFID channel connection, and the pilot computes a message response and sends it to the terminal as a response message, the response being a way function based on cryptographic hash computations, and the terminal establishing a secure short-range connection with the phone, and the terminal verifying the presence of a correct pilot by the terminal via computing and comparing an expected response from the mobile phone with the transferred security key.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- **Fox et al. (US 5943624)** - This invention relates to smartcard electronic devices and, more particularly, to the incorporation of smartcard devices in a cellular telephone for enhanced verification, security and accessibility to data stored on the smartcard.
- **Pertilla et al. (US 20040243519)** - This invention relates in general to communications, and more particularly to a system, method and apparatus for processing electronic commerce involving radio communication technology.

6. Any comments considered necessary by Applicant must be submitted no later that the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

7. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Evens Augustin whose telephone number is (571) 272-

6860. The Examiner can normally be reached on Monday-Friday from 10:00 AM-7:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Fischer, can be reached at (571) 272-6779.

Evens Augustin

October 27th, 2006

AJ Fischer 10/30/06

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600